AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A system of securely using decryption keys during configuration of an integrated circuit having programmable logic, comprises:

a microcontroller within the integrated circuit for receiving an encrypted bitstream;

a key storage register coupled to the microcontroller for storing key data;

a decryptor coupled to the key storage register, wherein only the decryptor reads from the key storage register; and

a configuration data register in the integrated circuit, wherein the configuration data register is readable by the microcontroller before the decryptor is used and the configuration data register cannot be read by the microcontroller after the decryptor is used,

wherein the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware, independent of the microcontroller, that allows the microcontroller access to the key storage register by unblocking a signal path coupling the microcontroller and the key storage register when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory and disallows the microcontroller access to the key storage register by blocking the signal path coupling the microcontroller and the key storage register.

2-4. (Cancelled)

5. (Previously Presented) The system of claim 1, wherein the memory is a ROM having a decryption engine.

6. (Previously Presented) The system of claim 1, wherein the microcontroller further receives a configuration boot program comprising the decryptor in programmatic form along with the encrypted bitstream comprising encrypted configuration data to be loaded into the configuration data register.

7. (Previously Presented) The system of claim 1, wherein the microcontroller, the key register, the decryptor, and the configuration data register are all within the integrated circuit.

8. (Previously Presented) The system of claim 1, wherein the microcontroller is an emulated microcontroller in the integrated circuit.

9. (Currently Amended) A system of securely using decryption keys during configuration of an integrated circuit having programmable logic, comprising:

a microcontroller within the integrated circuit for receiving an encrypted bitstream;

a key storage register coupled to the microcontroller for storing key data;

a decryption program stored in a memory that uses a predetermined memory address to enable access to the key storage register; and

a configuration data register in the integrated circuit, wherein the configuration data register is readable by the microcontroller before the decryption program is used and the configuration data register cannot be read by the microcontroller after the decryption program is used;

wherein access to the key storage register by the microcontroller is allowed only when a program counter of the microcontroller specifies an address within an address range corresponding to the decryption program in the memory by unblocking a signal path coupling the microcontroller and the key storage register,

wherein access to the key storage register by the microcontroller is disallowed when the program counter of the microcontroller specifies an address outside of an address range corresponding to the decryption program in the memory by blocking the signal path coupling the microcontroller and the key storage register.

10. (Original) The system of claim 9, wherein the memory is a ROM containing a decryption engine.

11. (Original) The system of claim 9, wherein the microcontroller further receives a configuration boot program along with the encrypted bitstream.

12. (Currently Amended) A method of securely using decryption keys during configuration of an integrated circuit comprising programmable logic, comprising the steps of:

receiving an encrypted bitstream at a microcontroller within the field programmable gate array;

loading a decryptor with data from a key register;

loading the decryptor with data from the microcontroller;

loading a configuration data register with a decrypted bitstream from the decryptor, wherein the configuration data register is readable by the microcontroller before the decryptor is used and the configuration data register cannot be read by the microcontroller after the decryptor is used;

enabling access to the key register by unblocking a signal path coupling the microcontroller and the key register only when a program counter of the microcontroller specifies an address within an address range of the decryptor; and

disabling access to the key register by blocking the signal path coupling the microcontroller and the key register when the program counter of the microcontroller specifies an address outside of the address range of the decyptor.

13. (Original) The method of claim 12, wherein the method further comprises the step of loading the key register with key data from the microcontroller.

14. (Previously Presented) The method of claim 12, wherein the configuration data register cannot be read by the microcontroller while the decryptor is used.

15. (Original) The method of claim 12, wherein the microcontroller cannot read from the key register.

16. (Previously Presented) The method of claim 12, wherein only the decryptor can read from the key register.

17-19. (Cancelled)

20. (Currently Amended) A computer-readable medium comprising instructions written thereon in the form of a bitstream that configures an integrated circuit comprising programmable logic, the computer-readable medium comprising:

a configuration boot program portion of the bitstream that runs a microcontroller on the integrated circuit; and

an encrypted bitstream portion of the bitstream containing encrypted configuration data that when decrypted and loaded into a configuration data register on the integrated circuit configures the programmable logic,

wherein the configuration boot program further comprises instructions for a decryptor, wherein the configuration boot program stores the instructions for the decryptor in a memory, wherein the decryptor is executed by a microcontroller and decrypts the encrypted bitstream using key data stored within a key storage register, and wherein access to the key storage register by the microcontroller is selectively permitted by blocking or unblocking a signal path coupling the microcontroller to the key storage register according to whether a program counter of the microcontroller specifies an address within an address range corresponding to the decryptor within the memory.

wherein the decryptor loads the configuration data register with the decrypted bitstream, the configuration data register is readable by the microcontroller before the decryptor is used, and the configuration data register cannot be read by the microcontroller after the decryptor is used.

21. (Cancelled)

22. (Previously Presented) The computer-readable medium of claim 20, wherein the configuration boot program comprises instructions for a decompressor.